IoT Based RPL Routing Protocol Improvement against DDoS Cyber Attack Using NetSim v14.1 Simulation Program

Shayma Wail Nourildean[1,*], Mohammed Joudah Zaiter[2], Mustafa Dhia Hassib[1], and Yousra Abd Mohammed[1]
[1] University of Technology- Iraq
[2] Electrical Engineering Technical College, Middle Technical University, Baghdad, Iraq
Email: Shayma.w.nourildean@uotechnology.edu.iq (S.W.N.), mjzaiter@yahoo.com (M.J.Z.), mustafa.d.hassib@uotechnology.edu.iq (M.D.H.), Yousra.A.Mohammed@uotechnology.edu.iq (Y.A.M.)

Manuscript received September 20, 2024; revised November 21, 2024; accepted December 4, 2024
*Corresponding author

***Abstract*—The Internet of Things (IoT) is a developing technology that can enhance the communication capabilities of Wireless Sensor Networks (WSN) when integrated together. The nature of IoT networks is characterized by self-organization and decentralization, leading to changes in the nodes' position. Therefore, routing in the IoT is essential for the successful transmission of data. RPL (routing protocol for low-power and lossy networks) was evaluated for IoT objects. This paper's aim is to examine the efficiency of IoT based on RPL as a routing protocol when bit and piece distributed denial-of-service (DDoS) cyber attack mitigate the traffic into the network. Cyber attacks had affect any IoT network by increasing the delay, jitter and reducing the throughput resulting in degradation in IoT network performance. Bit and piece DDoS is taken in this paper as an example of any cyber attack, other types could be taken like malware, phishing with the affect the IoT performance also. This simulation is done in number of NetSim verified scenarios in terms of throughput, delay, Jitter, packet delivery rate and bit error rate Quality of Service (QoS) parameters. The results show that RPL when applied to the IoT network investigated a better QoS improvement than any Ad-Hoc Routing Protocol like (AODV). The improvement had been investigated by increasing the throughput and decreasing the delay, Jitter and BER which are the QoS parameters taken in this paper.**

***Index Terms*—IoT, sensors, RPL, NetSim, QoS, cyber attack**

I. Introduction

Internet of Things (IoT) refers to a network where physical objects, equipment, sensors, and other items have autonomous communication with each other without the need for human intervention [1]. The IoT is a prominent regional framework that involves the characteristic elements of a traditional system, enabling communication and data exchange between interconnected devices [2]. The IoT is a developing technology that can enhance the communication capabilities of Wireless Sensor Networks (WSN) when integrated together [3, 4]. WSN is a crucial element of the IoT, and it has expanded to various applications in real time. The WSNs and IoT have a wide range of applications that affect almost every aspect of our daily lives, both in terms of essential and non-essential functions [1]. Connecting electrical items to the Internet and fulfilling the connectivity and addressing needs is made simple by this technology [5]. The nature of IoT networks is characterized by self-organization and decentralization, leading to dynamic changes in the position of nodes. Therefore, routing in the IoT is essential for the successful transmission of data [6]. RPL (routing protocol for low-power and lossy networks) and it was evaluated to the stationary IoT objects [7]. Cybersecurity observes current and relevant information related to the latest Information Technology data. Researchers around have suggested many methodologies to avoid cyber attacks and minimize their effects [8]. The aim of this paper is to study the effect of bit and piece DDoS (distributed denial of service) cyber attack to the performance of network in terms of throughput, delay, bit error rate (BER) and packet delivery rate (PDR). This paper utilized RPL as a routing protocol in the IoT network and compared the performance of this network based on RPL with any ad hoc routing protocol like AODV (ad hoc on-demand distance vector routing) [9]). This study is done in number of valuable scenarios using NetSim v14.1 which is a specific simulation program for any IoT network.

II. Related Work

IoT is an emerging technology which it is integrated in everyday life, many studies had been examined in the RPL routing protocols. Shimaa A. Abdel Hakeem and her colleagues suggested a practical and simulated application of RPL behavior, making necessary adjustments to meet the routing needs of WSN. The Cooja implementation findings revealed that numerous RPL nodes experienced significant packet loss rates, network congestion, and frequent retransmissions as a result of selecting pathways with highly unreliable links [10]. Harith Kharrufa *et al.* provided a RPL key elements analysis. They evaluate and contrast RPL protocols in terms of their reliability, flexibility, robustness, security and efficiency. They determined the potential future paths of RPL and its suitability in the future Internet [11].

doi: 10.18178/ijeetc.14.1.35-42

Khalid Darabkh *et al.* presented an extensive overview of the functioning of the RPL protocol, using innovative and meticulous illustrations. This paper provides an overview and analysis of RPL-based protocols, focusing on their robustness, energy efficiency, adaptability and dependability [12]. Khalid A. Darabkh *et al.* had successfully addressed the issues faced by IoT researchers and their contribution to improving the RPL protocol. They have approached these challenges in an effective manner. This paper would be interested to all researchers in the field of RPL [13]. Sangeeta Rani *et al.*. conducted a comprehensive study on various load balancing schemes, matrices, objective functions, and RPL-based routing protocols. The survey specifically focused on the representation and highlighting of load imbalance when load balancing is integrated with RPL, and the significant influence it made. The RPL-based organizing show, its presenting decisions, and the limits were thoroughly examined [14]. Ibrahim S. Alsukayti *et al*. conducted a comprehensive experimental study on critical RPL routing attacks. The study examined various attack scenarios in RPL network setups of different scales. The findings revealed that the targeted networks suffered significant degradation in Quality of Service (QoS) performance and stability of their topology [15]. Karen Avila *et al*. conducted a study on the attacks in RPL and the methods used to prevent them. They conducted a systematic literature review (SLR) following the Massaro technique. In addition, they establish the primary authors and countries that require more improvement in this area of research [16]. Xiyuan Liu *et al*. conducted a study focused on analyzing the performance of RPL in multi-hop networks of significant scale, utilizing the OMNeT++ simulation framework. The discussion has also addressed the difficulties associated with the deployment and security of applications posed by RPL. The research findings will serve as a significant reference for network engineers aiming to develop more efficient routing algorithms for IoT applications [17]. Bandarupalli Rakesha and H. Parveen Sultanab analyze the constraints of the RPL protocol in data routing and examine the solutions put forth by many researchers. They also evaluate the disadvantages of the methodology given by these researchers. Based on our analysis, we have determined that there are numerous opportunities to improve security and enhance the Quality of Service (QoS) [18]. Saurav Kumar and Ajit kumar Keshrithe presented an Optimization-Based Adaptive Security in this paper offering a potent solution for mitigating DDoS attacks in IoT environments. Through dynamic adjustment of security measures based on real-time threat analysis, the model exhibits robust defense posture and resilience against a variety of DDoS attack scenarios. Integrated with MATLAB and employing optimization techniques, this model demonstrates promising results in bolstering IoT security [19]. Jesús Galeano-Brajones *et al*., propose to experimentally evaluate an entropy-based solution to detect and mitigate DoS and DDoS attacks in IoT scenarios using a stateful SDN data plane. The obtained results demonstrate for the first time the effectiveness of this technique targeting real IoT data traffic [20].

This paper improves the previous works by introducing the effect of bit and piece DDoS cyber attack on IoT network and how RPL can improve the throughput, delay, BER and PDR compared with any ad hoc routing protocol like AODV. The NetSim v14.1 had been utilized as a simulation tool which it is a specific tool for IoT network.

III. Theoretical Basis

A. Internet of Things (IoT)

The IoT refers to a network of physical items that are equipped with electronic embedded technology. These devices are capable of communicating, sensing, and interacting with their internal states as well as the external world. The IoT is a worldwide network infrastructure that is capable of configuring itself and uses standard and interoperable communication protocols. In this network, both virtual and physical objects have unique identities, physical characteristics, and virtual personalities. These objects also have intelligent interfaces and are smoothly incorporated into the network. The IoT enables seamless connectivity between individuals, objects, and networks, regardless of location, by utilizing various paths, networks, and services [21]. The primary impact of the IoT is the persistent integration of various things, such as Radio Frequency Identification (RFID) tags, sensors, actuators, and mobile phones. These objects own unique addressing systems and have the ability to perceive and collaborate with each other in order to achieve common objectives [22]. These sensors including as environmental monitoring sensors, temperature sensors, home appliances and security cameras. These repositories store and accumulate the data, making it accessible to authorized users. However, the impact of IoT-based traffic on network efficiency is typically not significant due to the fact that every IoT object transmits data to a dedicated IoT server. Consequently, the data generated by numerous objects may have a cumulative effect on network performance. Thus, in the absence of human intervention, the IoT networks will operate securely and efficiently for an extended period of time [1].

B. Wireless Sensor Network

WSNs serve as the primary means of data collection for IoT devices. IoT based on WSN is a network of multiple small sensors that are spread out in different locations and powered by batteries. These sensors work together to perform a certain task [23]. Every device operates with a battery that has a finite amount of energy. In addition, these devices possess limited computational capabilities, as well as restricted sensing and transmission capabilities. The longevity of a node is contingent upon the energy stored in its battery. The IoT heavily relies on WSNs [24]. WSN play a vital role in the expansion and advancement of the IoT as they allow inexpensive devices with restricted capabilities to connect to revolutionary applications [25]. In IoT- WSNs, sensors constantly observe the environment and notify the Base Station (BS) upon detecting any occurrence. Then it is

equipped with a gateway that facilitates the uploading of the gathered data to the IoT Cloud. Users have the ability to view the IoT data stored in the Cloud remotely at their convenience. Several applications of IoT-based WSNs include healthcare systems [26], smart irrigation, smart cities, and smart buildings [24]. WSN architecture is illustrated in Fig. 1.

Fig. 1. Architecture of wireless sensor networks [27].

C. IoT Routing Protocols

The advent of the IoT allows for the seamless connectivity of smart devices embedded in various objects, enabling them to be linked to any network, any service, and any individual or entity, regardless of time or location. IoT networks exhibit self-organizing and decentralized characteristics, leading to nodes' position dynamic changes. Therefore, routing in the IoT is essential for the successful transmission of data. The constrained energy and processing capabilities of connected devices provide significant challenges for routing in IoT networks [28]. Multiple routing protocols have been developed specifically for efficient operation in IoT networks, in order to address the many obstacles presented by the limited resources and conditions of the environment [28]:

1) The Collection Tree Protocol (CTP).
2) RPL protocol.
3) LOADing protocol.
4) Develop an expansion for the collection tree protocol.

IETF has recently established the IPv6 Routing Protocol (RPL) as a standard for LLNs. This protocol has gained widespread acceptance throughout the Internet community. Low power lossy IoT network is shown in Fig. 2 [6].

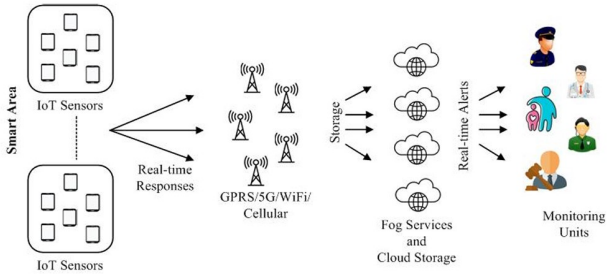


Fig. 2. Low power and lossy IoT network [6].

D. RPL

RPL is a routing protocol that is specifically developed for low power devices using IPv6. It functions on IEEE 802.15.4 standard and it is supported by the 6LoWPAN adaptation layer. The RoLL working group introduced routing requirements for LLNs, considering the limited energy resources, processing, and memory. The goal is to enable a large number of peer to peer nodes to communicate. The RPL protocol effectively and optimally handles the routing of data for nodes with limited resources. It offers a framework that guarantees two-way connectivity, strength, dependability, adaptability, and scalability [11]. RPL operates in a proactive manner. The system facilitates several communication techniques, including point-to-point, point-to-multipoint, and multipoint-to-point. Hence, RPL offers the necessary assistance to fulfill the diverse needs of a wide array of IoT applications [15].

E. AODV (Ad Hoc on-Demand Distance Vector)

It is a popular routing protocol designed for use in any wireless networks where the network topology frequently changes. It enables dynamic, self-starting, and efficient routing between mobile nodes. AODV builds routes only when they are needed, which reduces overhead compared to table-driven routing protocols that maintain routes continuously. It is suitable for small- to medium-sized networks, AODV can handle moderate network sizes efficiently [29].

F. Cyber Attacks

Cyber attacks aim to cause financial damage to companies. Cyber-attacks can, in certain instances, serve military or political objectives [8]. Cyberattack is a kind of attack that targets computer or computer network in an attempt to steal, alter or destroy any critical data present in it [30]. Examples of these damages encompass PC viruses, Data Distribution Service (DDS), knowledge breaches, and other avenues of assault. Various businesses adopt diverse techniques to reduce damage resulting from cyber-attacks. Cybersecurity observes current and relevant information related to the latest Information Technology data. Researchers around have suggested several methodologies to preempt cyber-attacks or alleviate their effects [8]. The attacker could be any process or people that obtains illegal access or usage. The various types of cyber attacks include DoS and DDoS attacks, phishing attacks, malware attacks, man-in-the-middle (MitM) attacks, drive-by-download attacks, SQL injection attacks, password attacks, cross-site scripting (XSS) attacks, eavesdropping attacks and birthday attacks [30].

G. Bit and Piece DDoS

The bit and piece DDoS attack is a recently discovered and disclosed attacking technique by nexusguard. This assault primarily focuses on communication service providers and involves the insertion of undesirable and irrelevant data into legitimate network traffic, hence avoiding detection methods. Fig. 3 illustrates the bit-and-piece attack architecture. The bit-and-piece attack

involves the attacker gaining control over multiple local systems by exploiting vulnerabilities in the internet service provider (ISP). The assailant transmits the offensive directives via ISP. The local systems connected to ISP's are being targeted by cyberattacks orchestrated by a mastermind [31].

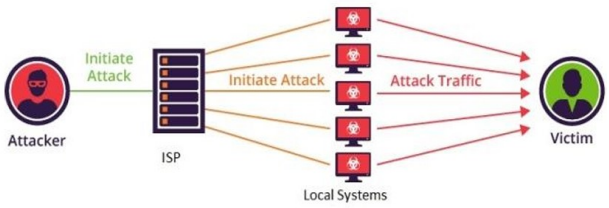


Fig. 3. Bit-and-piece attack structure.

IV. Research Method

This paper aimed to examine the IoT performance based on RPL Routing protocol with and without cyber-attack. This IoT network is based on WSN including number of sensor nodes connecting via 6LoPWAN gateway to the cloud which can be accessed by any user. Then the bit and piece DDoS cyber-attack mitigate the traffic into the network causing performance and reliability degradation so that the paper examine the throughput, delay, jitter, packet delivery rate and bit error rate QoS parameters of IoT based on RPL routing protocol when it is compared with any ad hoc network like AODV. The impact of a DDoS attack on IoT networks can be devastating, leading to severe network congestion that disrupts both real-time and non-real-time traffic. High latency, jitter, and BER can compromise the functionality of IoT applications, with critical services being especially vulnerable. Ensuring robust DDoS mitigation strategies, such as traffic filtering, load balancing, and anomaly detection, is essential for maintaining the stability and reliability of IoT networks. The simulation paper is done using NetSim v14.1 in number of different modeled scenarios as follows.

Case 1:

- Drop 9 sensors, 1 6LoWPAN gateway, 1 router, and 1 wired node as shown in Fig. 4.
- Set the routing protocol to RPL and AODV in the sensors.
- Set wireless link channel characteristics as path loss only.
- Pathloss model=Log distance with pathloss exponent = 4.5.
- Configure traffic from all sensors 1 through 8 such that the packets are transmitted to the gateway via sensor 9. The traffic rate is low; it is 20 packets per second.
- Run the simulation for 100 seconds and measure the throughput obtained by sensors 1 through 8.

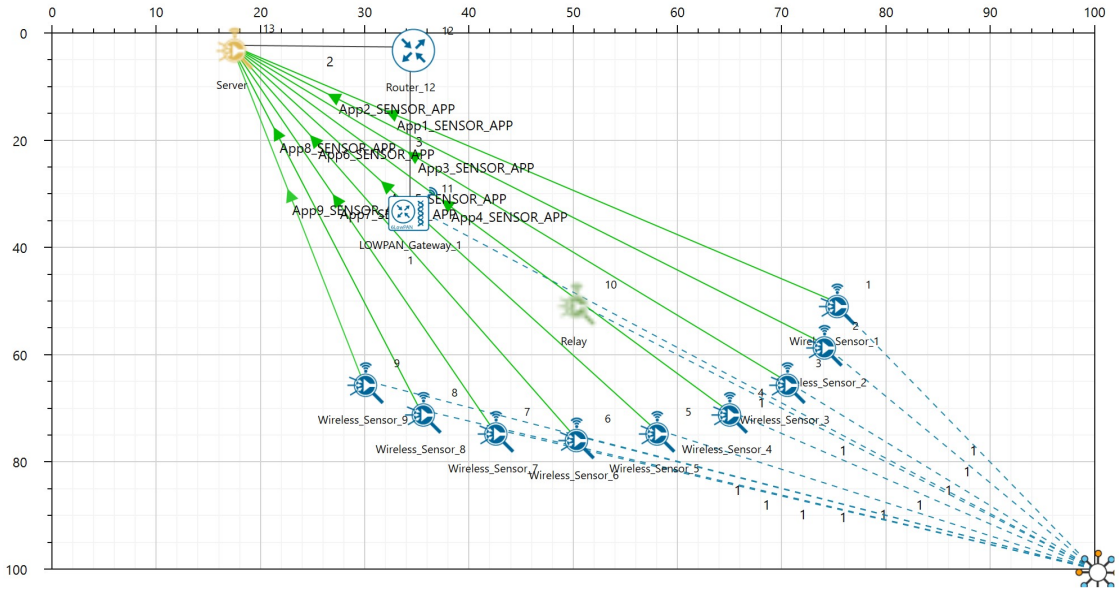


Fig. 4. IoT network without malicious node.

Case 2:

- Add 3 malicious nodes (wired). Configure traffic from 3 malicious nodes to all sensors (1, 2, ···, 9). Packets of size 10 bytes (representing a small amount of attack data) are sent at a rate of 20 packets/sec exponentially as shown in Fig. 5
- Set the routing protocol to RPL and AODV in the sensors.
- Set wireless link channel characteristics as path loss only.
- Pathloss model = log distance with pathloss exponent = 4.5.
- Configure traffic from all sensors 1 through 8 such that the packets are transmitted to the gateway via sensor 9. The traffic rate is low; it is 20 packets per second.
- Run the simulation for 100 seconds and measure the throughput obtained by sensors 1 through 8.

Evaluation Metrics:

- *Throughput*: The actual rate measured in bits per second (bps), at which data is successfully transferred over a communication channel. It indicates the performance of a network, showing how much data can be transmitted successfully in a given time frame.
- *Delay (Latency)*: The time measured in milliseconds (ms) it takes for a packet of data to travel from the source to the destination across a network. Lower latency is generally better for performance.
- *Jitter*: The variation in the time delay Measured in milliseconds (ms)between packets arriving at the destination. Inconsistent packet delay can cause issues in streaming or real-time applications. High jitter can lead to degraded performance in real-time applications
- *Bit Error Rate (BER)*: The number of bit errors per unit of time or per number of bits transmitted, received, or processed. It expressed as a ratio, such as 1 error in 1 million bits (1E-6). BER is an important measure of the quality of a communication link. A lower BER indicates a higher quality and more reliable communication channel.

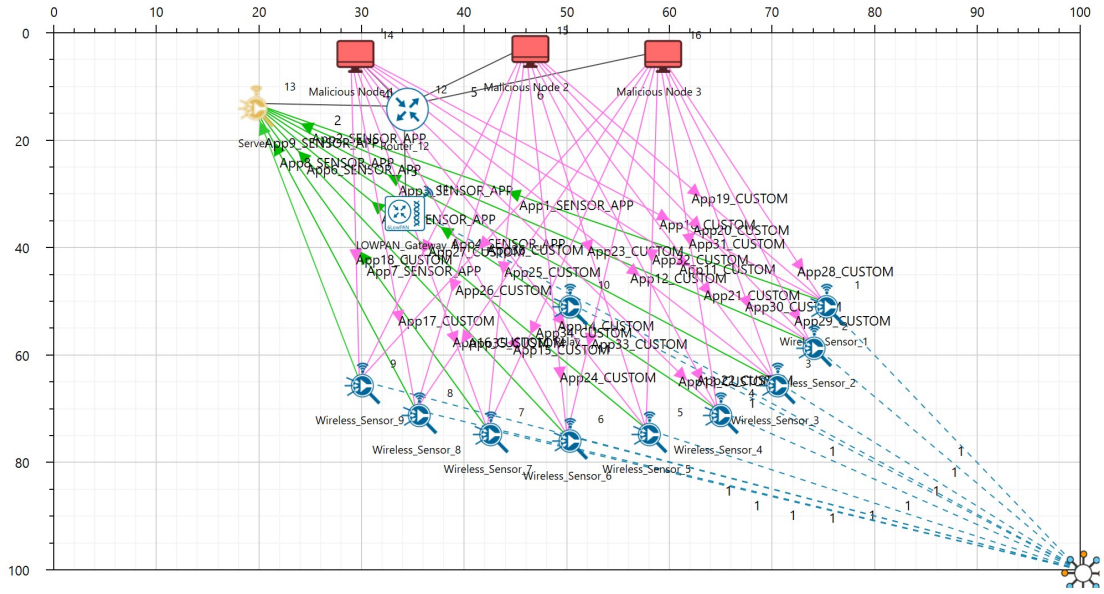


Fig. 5. IoT network with malicious nodes.

V. Results and Discussion

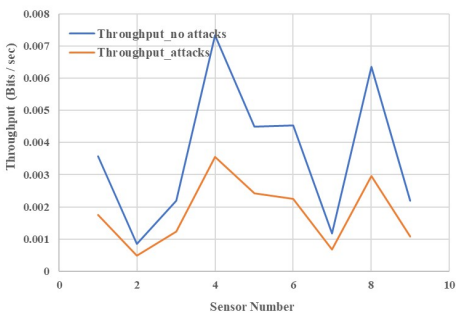
Throughput, Delay, Jitter, Bit Error Rate (BER) and PDR QoS parameters had been collected for IoT network when RPL and AODV routing protocols are applied to examine the improvement of RPL over AODV in the IoT with bit and piece cyber attack as follows:

1) Throughput, Delay, PDR and BER are taken for the IoT network with and without attacker to examine the degradation in IoT efficiency as shown in Fig. 6.

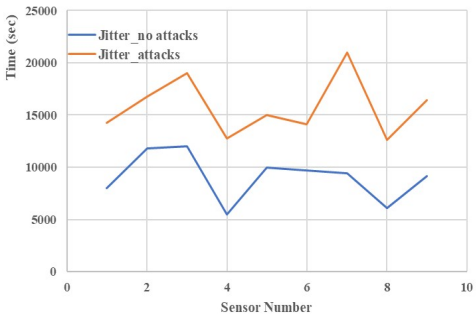
As shown in Fig. 6, the bit and piece attack had degraded the IoT Network performance by decreasing throughput and PDR and increasing delay, Jitter and BER which affect the efficiency and reliability of the network which it is indicated by the increasing of BER.

2) Throughput, Delay, PDR and BER are taken for the IoT network with attacker when RPL routing protocol and AODV ad hoc routing protocol to examine the improvement caused by RPL over AODV as shown in Fig. 7.

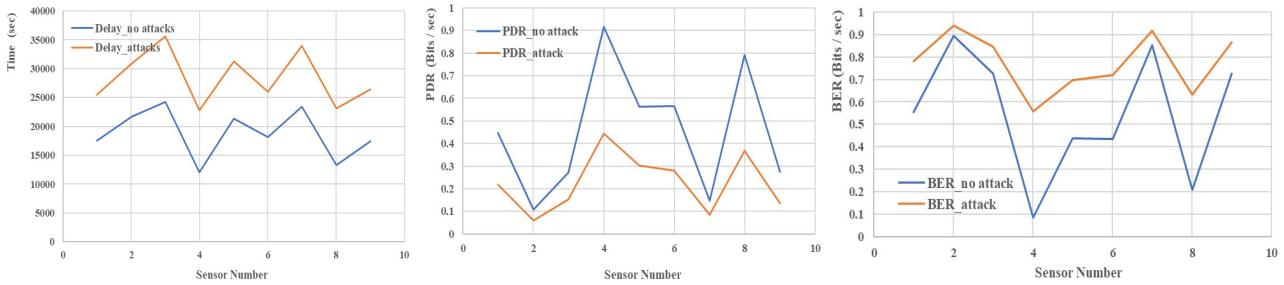
As shown in Fig. 7, the number of bits transmitted per second, the rate of packet delivered IoT network when RPL routing protocol is used are larger than AODV, and the delay, jitter and bit error rate are decreased so that this is a good improvement of RPL over any ad hoc routing protocol like AODV which improved throughput, packet delivery rate and the reliability of the network.



(a)

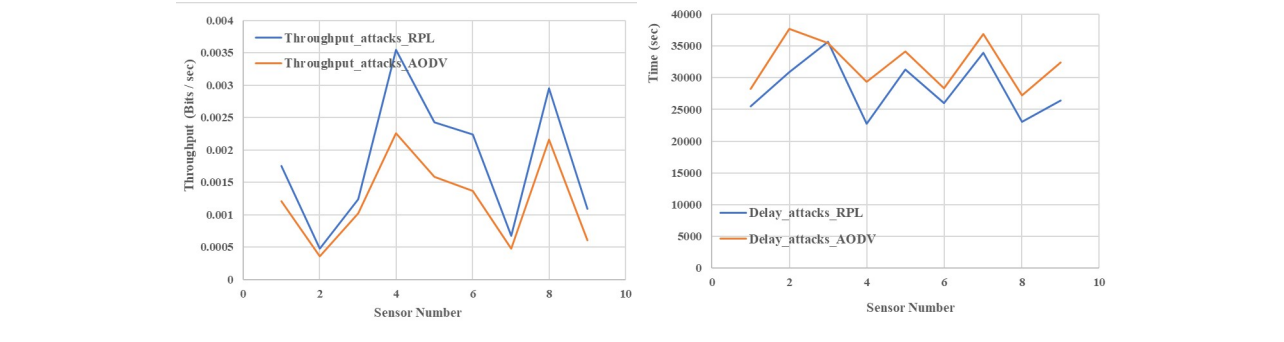


(b)

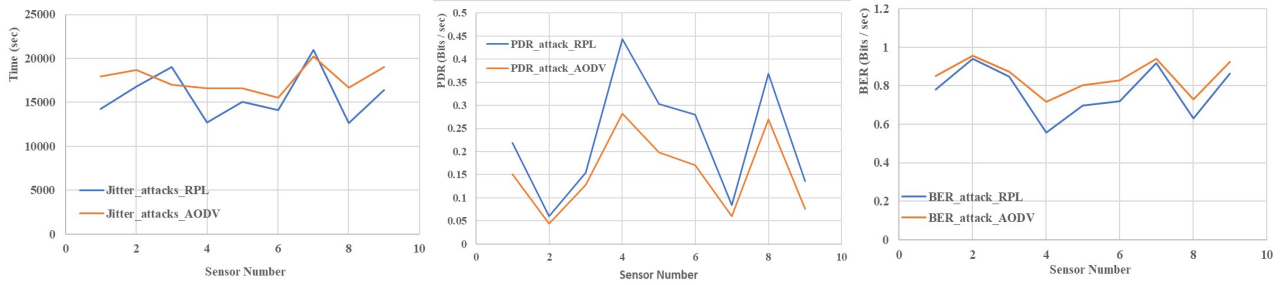


(c) (d) (e)

Fig. 6. QoS parameters of IoT with and without attack: (a) Throughput, (b) delay, (c) jitter, (d) PDR, and (e) BER.



(a) (b)



(c) (d) (e)

Fig. 7. QoS parameters of IoT based on RPL and AODV routing protocols: (a) Throughput, (b) delay, (c) jitter, (d) PDR, and (e) BER.

VI. Conclusion

Routing in the IoT is essential for the successful transmission of data. RPL is a routing protocol that is specifically developed for low power devices using IPv6. It functions on the IEEE 802.15.4 standard and is supported by the 6LoWPAN adaptation layer. The aim of this paper is to examine the IoT network performance based on RPL as a routing protocol when bit and piece DDoS cyber attack mitigate the traffic into the network. In this paper, nine sensors are connected to 6 LoWPAN gateway to the cloud to be accessed from any user. Two routing protocols (RPL and AODV) had been applied to each sensor node in the IoT network. The performance of network had been measured in terms of five Quality of Service parameters (Throughput, delay, Jitter, PDR and BER). The simulation is done using Netsim v14.1 simulation program so that the results showed that the DDoS cyber attack affect the IoT network performance by decreasing throughput and packet delivery rate and increasing delay, Jitter and bit error rate. The IoT based on RPL routing protocol had larger throughput and PDR as well as less delay, Jitter and BER than IoT based on AODV which is taken in this paper as an ad hoc routing protocol. It can be concluded from this paper that RPL routing protocol had improved the throughput, the rate of packets delivered and the reliability of IoT network and reduced the degradation in IoT network performance caused by the DDoS cyber attack. The impact of a DDoS attack on IoT networks can be devastating, leading to severe network congestion that disrupts both real-time and non-real-time traffic. High latency, jitter, and BER can compromise the functionality of IoT applications, with critical services being especially vulnerable. Ensuring robust DDoS mitigation strategies, such as traffic filtering, load balancing, and anomaly detection, is essential for maintaining the stability and reliability of IoT networks. The future work might include different types of cyber attacks which affect any IoT network or the study of RPL protocol improvement for any Mobile Ad Hoc Networks (MANET).

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

Shayma W. Nourildean and Mohammed J. Zaiter conducted the research and analyzed the data; Shayma W.

Nourildean and Mustafa D. Hassib wrote the drafted paper; all authors had approved the final version.

REFERENCES

[1] K. Gulati, R. S. Kumar Boddu, D. Kapila, S. L. Bangare, N. Chandnani, and G. Saravanan, "A review paper on wireless sensor network techniques in Internet of Things (IoT)," *Mater. Today Proc.*, vol. 51, pp. 1–5, 2021. doi: 10.1016/j.matpr.2021.05.067

[2] A. H. Bagdadee, M. Z. Hoque, and L. Zhang, "IoT based wireless sensor network for power quality control in smart grid," *Procedia Comput. Sci.*, vol. 167, no. 2019, pp. 1148–1160, 2020. doi: 10.1016/j.procs.2020.03.417

[3] A. Gupta, T. Gulati, and A. K. Bindal, "WSN based IoT applications: A review," *Int. Conf. Emerg. Trends Eng. Technol. ICETET*, vol. 2022-April, 2022. doi: 10.1109/ICETET-SIP-2254415.2022.9791495

[4] S. W. Nourildean and M. D. Hassib, "IoT-based MANET performance improvement against jamming attackers in different mobile applications," *e-Prime - Adv. Electr. Eng. Electron. Energy*, vol. 8, 2024. doi: 10.1016/j.prime.2024.100615

[5] A. Hendra, E. Palantei, Syafaruddin, M. S. Hadis, N. Zulkarnaim, and M. F. Mansyur, "Wireless sensor network implementation for IoT-based environmental security monitoring," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 875, no. 1, pp. 1–5, 2020. doi: 10.1088/1757-899X/875/1/012093

[6] Z. Shah, A. Levula, K. Khurshid, J. Ahmed, I. Ullah, and S. Singh, "Routing protocols for mobile Internet of Things (IoT): A survey on challenges and solutions," *Electron.*, vol. 10, no. 19, pp. 1–29, 2021. doi: 10.3390/electronics10192320

[7] M. Pahuja and D. Kumar, "Taxonomy of various routing protocols of IoT-based on wireless sensor networks for healthcare: Review," *Int. J. Comput. Networks Appl.*, vol. 10, no. 4, pp. 569–602, 2023. doi: 10.22247/ijcna/2023/223314

[8] Y. Li and Q. Liu, "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments," *Energy Reports*, vol. 7, pp. 8176–8186, 2021. doi: 10.1016/j.egyr.2021.08.126

[9] S. W. Nourildean, M. D. Hassib, and Y. A. Mohammed, "Ad-Hoc routing protocols in WSN-WiFi based IoT in smart home," in *Proc. International Conference on Developments in eSystems Engineering, DeSE*, 2023, pp. 82–87. doi: 10.1109/DeSE58274.2023.10099981

[10] S. A. A. Hakeem, A. A. Hady, and H. W. Kim, "RPL routing protocol performance in smart grid applications based wireless sensors: Experimental and simulated analysis," *Electron.*, vol. 8, no. 186, pp. 1–23, 2019. doi: 10.3390/electronics8020186

[11] H. Kharrufa, H. A. A. Al-Kashoash, and A. H. Kemp, "RPl-based routing protocols in IoT applications: A review," *IEEE Sens. J.*, vol. 19, no. 15, pp. 5952–5967, 2019. doi: 10.1109/JSEN.2019.2910881

[12] K. A. Darabkh, M. Al-Akhras, and M. A. Jumana N. Zomot, "RPL routing protocol over IoT: A comprehensive survey, recent advances, insights, bibliometric analysis, recommendations, and future directions," *J. Netw. Comput. Appl.*, vol. 207, 2022.

[13] K. A. Darabkh and M. Al-Akhras, "RPL over Internet of things: challenges, solutions, and recommendations," in *Proc. 2021 IEEE International Conference on Mobile Networks and Wireless Communications, ICMNWC 2021*, 2021. doi: 10.1109/ICMNWC52512.2021.9688375

[14] S. Rani, A. Kumar, A. Bagchi, S. Yadav, and S. Kumar, "RPL based routing protocols for load balancing in IoT network," *J. Phys. Conf. Ser.*, vol. 1950, no. 1, pp. 1–11, 2021. doi: 10.1088/1742-6596/1950/1/012073

[15] I. S. Alsukayti and M. Alreshoodi, "RPL-based IoT networks under simple and complex routing security attacks: An experimental study," *Appl. Sci.*, vol. 13, no. 8, pp. 1–23, 2023. doi: 10.3390/app13084878

[16] K. Avila, D. Jabba, and J. Gomez, "Security aspects for Rpl-based protocols: A systematic review in IoT," *Appl. Sci.*, vol. 10, no. 18, pp. 1–20, 2020. doi: 10.3390/APP10186472

[17] X. Liu, Z. S. C. Yin, F. Ali, and D. Roggen, "Performance analysis of routing protocol for low power and lossy networks (RPL) in large scale networks," *IEEE Internet Things J.*, pp. 1–14, 2023. doi: 10.1007/978-3-031-24848-1_25

[18] B. Rakesh and H. P. Sultana, "A review on enhanced routing solutions in RPL protocol," *Int. J. Performability Eng.*, vol. 17, no. 11, pp. 938–945, 2021. doi: 10.23940/ijpe.21.11.p4.938945

[19] S. Kumar and A. Keshri, "An effective DDoS attack mitigation strategy for IoT using an optimization-based adaptive security model," *Knowledge-Based Syst.*, vol. 299, no. 5, p. 112052, Sep. 2024. doi: 10.1016/J.KNOSYS.2024.112052

[20] J. Galeano-Brajones, J. Carmona-Murillo, J. F. Valenzuela-Valdés, and F. Luna-Valero, "Detection and mitigation of DoS and DDoS attacks in iot-based stateful SDN: An experimental approach," *Sensors (Switzerland)*, vol. 20, no. 3, pp. 1–18, 2020. doi: 10.3390/s20030816

[21] H. Doshi and A. Shankar, "Wireless sensor network application for IoT-based healthcare system," in *Data Driven Approach Towards Disruptive Technologies*, T. P. Singh, R. Tomar, T. Choudhury *et al.*, Ed. Springer, Singapore. https://doi.org/10.1007/978-981-15-9873-9_24

[22] S. G. Fatima, S. K. Fatima, S. M. Ali, N. A. Khan, and S. Adil, "Methodologies and challenges of WSN for IoT," *Int. J. Adv. Res. Eng. Technol.*, vol. 10, no. 2, pp. 210–214, 2019. doi: 10.34218/IJARET.10.2.2019.020

[23] S. A. A. A. M. K. Abdulzahra and A. K. M. Al-Qurabat, "Optimizing energy consumption in WSN-based IoT using unequal clustering and sleep scheduling methods," *Internet of Things*, vol. 22, no. 100765, 2023.

[24] R. B. Pedditi and K. Debasis, "Energy efficient routing protocol for an IoT-based WSN system to detect forest fires," *Appl. Sci.*, vol. 13, no. 3026, pp. 1–22, 2023. doi: 10.3390/app13053026

[25] R. Bharathi, S. Kannadhasan, B. Padminidevi, M. S. Maharajan, R. Nagarajan, and M. M. Tonmoy, "Predictive model techniques with energy efficiency for IoT-based data transmission in wireless sensor networks," *J. Sensors*, vol. 2022, pp. 1–18, 2022. doi: 10.1155/2022/3434646

[26] T. Harshita, "Healthcare using wireless sensor networks in IoT," *Int. J. Res. Publ. Rev.*, vol. 04, no. 12, pp. 4839–4844, 2023. https://doi.org/10.55248/gengpi.4.1223.123413

[27] T. Jabeen, I. Jabeen, H. Ashraf, N. Z. Jhanjhi, A. Yassine, and M. S. Hossain, "An intelligent healthcare system using IoT in wireless sensor network," *Sensors*, vol. 23, no. 11, pp. 1–14, 2023. doi: 10.3390/s23115055

[28] D. Sharma, S. Jain, and R. Sharma, "A comprehensive review of routing protocols for internet of things," *Int. J. Eng. Trends Technol.*, pp. 1–7, 2020. doi: 10.17762/itii.v9i2.449

[29] S. W. Nourildean, S. I. Jasim, M. T. Abdulhadi, and M. M. Jaber, "Point coordination mechanism based mobile ad hoc network investigation against jammers," *Eastern-European J. Enterp. Technol.*, vol. 5, no. 9–119, pp. 45–53, 2022. doi: 10.15587/1729-4061.2022.265779

[30] J. M. Biju, N. Gopal, and A. J. Prakash, "Cyber attacks and its different types," *Int. Res. J. Eng. Technol.*, vol. 6, no. 3, pp. 4849–4852, 2019.

[31] T. Subburaj and K. Suthen, "Bit-and-piece DDoS attack detection based on the statistical metrics," *Int. J. Eng. Adv. Technol.*, vol. 9, no. 1s4, pp. 48–55, 2019. doi: 10.35940/ijeat.a1086.1291s419

Shayma W. Nourildean is a lecturer (a member of an academic staff) in Communication Engineering department in University of Technology (UOT), Baghdad – Iraq. She holds a M.Sc. degree in control and computer engineering with specialization in computer engineering since 2006 and she received B.Sc. degree in Computer Engineering from Baghdad University in 2002. Her research areas are computer networks,

data communication and wireless sensor networks. she published a number of papers in national and international journals and participated in multiple national and international conferences.

Mohammed Joudah Zaiter has master's degree in electronic engineering (2004) University of technology – Baghdad AL-Rasheed College of Engineering & Science (Iraq) and Ph.D. in communication engineering (2014) Universiti Tenaga Nasional (UNITEN), working in the Department of Computer Engineering Techniques / Electrical Engineering Technical College / Middle Technical University. He has experience in computer network, security, embedded systems and communication systems.

Mustada Dhia Hassib earned his Ph.D. in communication Engineering from the Department of Electrical, Electronic and System Engineering at the National University of Malaysia in 2014. Mustafa earned his bachelor's and master's degree in communication Engineering from the University of Technology (UOT), Baghdad, Iraq in 1991 and 2003. Mustafa is serving as a member of the academic staff at Communication Engineering Department. His research interested focus on modeling of wireless and mobile communication system & coding and information theories and optical communication.